DATA NETWORK ACCESS

This invention relates to a method of providing a connection between a user's terminal connected to a telephone network and a data network through an interface which is connected to both the telephone network and the data network. This invention also relates to an interface for providing such a connection service.

The most widespread data network in use at present is the well-known public Internet. User's computers operated by individuals from their homes or individuals belonging to a small organisation are usually connected to the Internet by a dial-up connection through a telephone network to an interface known as a point-of-presence. In presently known arrangements, the point-of-presence requires the user's computer to provide both a user name and password for authentication before it will connect the user's computer to the public Internet. Some users find it inconvenient to establish a user name and password before gaining access to the public Internet.

It will be well known that the so-called Point-to-Point Protocol (PPP) is a datalink protocol that allows IP traffic to be carried over serial lines. See, for example, Internet Engineering Task Force (IETF) Request For Comments (RFC) 1661. PPP provides for two types of password authentication, Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). See further, for example, IETF RFC 1334.

A typical Internet Service Provider (ISP) at the present time will thus permit a user to connect to the Internet by means of a connection over a telephone network to a so-called Network Access Server (NAS) using PPP. The NAS will then allow a connection to the Internet on condition that the user is authenticated.

If, for example, PAP authentication is utilised, the user will send a username and a plaintext password to the NAS. A process of authentication will then take place to ascertain whether or not that password is the valid password for the username in question. Authentication may, for example, take place through the use of a so-called Remote Authentication Dial In User Service (RADIUS) server. See yet further, for example, IETF RFC 2138. In this case, the NAS would pass the username and password to the RADIUS server and the RADIUS server would authenticate the username on the basis of comparing the password provided with

the stored password corresponding to that username. If the password provided and the stored password match, then the RADIUS server would indicate to the NAS that that user had been authenticated and that the NAS may validly provide the user's computer with a network address, to allow subsequent access to the network.

CHAP authentication is considerably more secure than PAP authentication in that it does not send the plaintext password over the PPP link. CHAP authentication instead relies upon a comparison of the results of a particular computation performed upon a user's password by the user's computer and, with for example a RADIUS server, upon the stored password by the RADIUS server.

It may be the case that a user's password is the not the only authenticated attribute upon which access to a data network depends. A number of other attributes are known. The above mentioned IETF RFC 2138, for example, recites a list of such attributes. It is to be noted however that it is there provided, as was the opinion before the advent of the present invention, that, in these circumstances, for any user to be allowed access, verification of the user's password must always take place.

It will thus be appreciated that since such present day authentication relies upon the user's username and password, the means of authentication must already have a record of the user's username and password. As mentioned above, to gain access to, for example, the public Internet would thus inconveniently require that a user have a pre-established relationship with an Internet Service Provider.

According to one aspect of this invention there is provided a method of providing a connection service between a terminal and a data network, said terminal being arranged to be connected to a telephone network and said telephone network being connected to said data network through an interface, said method comprising the steps of:

in response to said terminal dialling an interface telephone number from a terminal telephone number, creating a connection through said telephone network between said terminal and said interface;

said interface ascertaining said dialled interface telephone number from said telephone network;

said interface checking that said dialled interface telephone number is one of one or more valid interface telephone numbers associated with said connection service;

in the event that said dialled interface telephone number is one of said valid interface telephone numbers, said interface allocating a data network address to said terminal and transmitting said address to said terminal; and

said interface providing a connection between said terminal and said data network .

With this invention, a user's computer can thus be connected to a data network without verification of a user name or password being necessary. Authentication is instead advantageously carried out on the basis of the telephone number dialled by the user's terminal to gain access to the connection service.

According to another aspect of this invention, there is provided a method of providing a connection service between a terminal and a data network, said terminal being arranged to be connected to a telephone network and said telephone network being connected to said data network through an interface, said method comprising the steps of:

in response to said terminal dialling an interface telephone number from a terminal telephone number, said interface receiving a connection through said telephone network from said terminal;

said interface ascertaining said dialled interface telephone number from said telephone network;

said interface checking that said dialled interface telephone number is one of one or more valid interface telephone numbers associated with said connection service;

in the event that said dialled interface telephone number is one of said valid interface telephone numbers, said interface allocating a data network address to said terminal and transmitting said address to said terminal; and

said interface providing a connection between said terminal and said data network .

According to yet another aspect of the invention, there is provided a method of providing a connection service between a terminal and a data network, said terminal being arranged to be connected to an access network and said

access network being connected to said data network through an interface, said method comprising the steps of:

in response to said terminal calling an interface access network address from a terminal access network address, said interface receiving a connection through said access network from said terminal;

said interface ascertaining an access network connection route attribute from said access network;

said interface checking that said access network connection route attribute is one of one or more valid access network connection route attributes associated with said connection service;

in the event that said access network connection route attribute is one of said valid access network connection route attributes, said interface allocating a data network address to said terminal and transmitting said address to said terminal; and

said interface providing a connection between said terminal and said data network .

According to yet another aspect of the invention, there is provided an interface for providing a connection service between a terminal and a data network, said terminal being arranged to be connected to a telephone network and said telephone network being connected to said data network through said interface, said interface comprising:

means arranged to receive a connection through said telephone network from said terminal in response to said terminal dialling an interface telephone number from a terminal telephone number;

means arranged to ascertain said dialled interface telephone number from said telephone network;

means arranged to check that said dialled interface telephone number is one of one or more valid interface telephone numbers associated with said connection service;

means responsive to said checking means arranged to allocate a data network address to said terminal and transmitting said address to said terminal in the event that said dialled interface telephone number is one of said valid interface telephone numbers; and

means arranged to provide a connection between said terminal and said data network.

This invention will now be described in more detail, by way of example, with reference to the drawings in which:

Figure 1 is a block diagram of the components which are used to form a connection between a user's terminal and the public Internet in accordance with this invention; and

Figure 2 is a flow chart showing the operations which are used with the arrangement of Figure 1 to form a connection between the user's terminal and the public Internet.

Referring now to Figure 1, there is shown a user's terminal 1 which is connected to a public telephone network 2. The user's terminal 1 may be connected on a digital or ISDN (Integrated Services Digital Network) line or on an analogue line. Where the connection is on an analogue line, the user's terminal 1 is connected to the telephone network 2 through a modem.

The arrangement shown in Figure 1 also includes an interface known as a point-of-presence 3 comprising a network access server 4 and an authentication server 5. The point-of-presence 3 is connected to both the telephone network 2 and the public Internet 6. It will be appreciated that the public Internet 6 is shown by way of only one example of any number of such suitable data networks which might instead be connected to the network access server 4. By way of an alternative an authentication server 5 might perform authentication for more than one network access server 4, each such network access server 4 at the respective points-of-presence 3 being connected to a single such authentication server 5. Each of the servers 4 and 5 is a computer configured so as to provide the functionality described below. The authentication server 5 may, for example, be based upon a conventional RADIUS server, but modified in accordance with the invention. The network access server 4 includes a bank of modems for receiving calls on analogue lines.

By way of illustration, Figure 1 shows another user's computer 7 and also a further server computer 8 connected to the public Internet 6.

The telephone network 2 has a telephone service billing system 9. The operation of the billing system 9 will be described below.

The point-of-presence 3 is thus associated with an Internet Service Provider. The telephone network 2 and the point-of-presence 3 may be associated with the same operator or with different operators.

As is well-known, computers connected to the Internet can transmit messages to each other using Internet protocols. These include the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Computers connected to the Internet can also retrieve information pages stored on server computers, such as the server computer 8, using higher level protocols. Several higher level protocols have been established for retrieving information pages and these include the File Transfer Protocol (FTP) and the now very well-known Hypertext Transfer Protocol (HTTP). Pages which are transmitted using the Hypertext Transfer Protocol are stored using the well-known Hypertext Mark-up Language (HTML). In order to retrieve such pages, a user's computer needs a suitable browser such as the well-known Netscape browser. One particular combination of the public Internet 6 and server computers connected to it and from which such information pages may be retrieved has become known as the World Wide Web (WWW). Information pages which may be retrieved from such server computers are commonly known as Web pages.

As indicated above, connection service methods known at the present time involving authentication on the basis of a username and password require a username and password to be stored at the point-of-presence or otherwise to be available therefrom prior to any connection session. As will become clear, in accordance with the invention this inconvenience is avoided. No pre-existing record of a username and a password for each user is required.

As will be explained, authentication instead takes place on the basis of a dialled telephone number. This merely requires that a record of pre-arranged valid connection service access telephone numbers instead be stored. This might, for example, take place through the operator of the point-of-presence storing such an access telephone number at the point-of-presence and then offering a connection service through that access telephone number. Alternatively, a third party, by prior arrangement with the point-of-presence operator and the telephone network operator if different, might be assigned a connection service access telephone number which is then stored at the point-of-presence.

Referring now to Figure 2, there are shown the operations which are to be performed in providing a connection service for creating a connection between, for example, a user's terminal 1, and the public Internet 6.

In a first step 20, the user's terminal 1 dials a connection service access telephone number. This may, for example, be an ordinary local access telephone number or a special rate telephone number. The user of the user's terminal 1 may find it convenient to configure the terminal 1 with this dedicated telephone number. Alternatively, it may be possible to pre-configure the particular connection service access software used by the user's terminal 1 to call the desired telephone number.

Then, in a second step 21, the telephone network 2 forms a connection between the user's terminal 1 and the network access server 4 in the point-of-presence 3. It will be appreciated that this may occur in a number of ways. In the first place, the telephone number called by the user's terminal 1 may simply connect directly with the network access server 4. Alternatively, by prior arrangement, the telephone network 2 may be configured such that, when a user's terminal 1 calls the dialled telephone number, the telephone network 2 associates the called number with a different telephone number. The connection with the network access server 4 may then be completed using this different telephone number. Such number translation functionality will be known from the International Telegraph and Telephone Consultative Committee (CCITT) Common-Channel Signalling System No.7. It will be further appreciated that, for example, a number of such dedicated telephone numbers may be translated into a single access telephone number for the network access server 4.

Once the call initiated by the user's terminal 1 has been connected to the network access server 4, the network access server 4 then proceeds in a third step 22 to ascertain the telephone number to which the user's terminal 1 placed the call. Such dialled number functionality, commonly referred to as Dialled Number Information Service (DNIS), will be known from the International Telegraph and Telephone Consultative Committee (CCITT) Common-Channel Signalling System No.7.

It is to be noted that it may be the case that one of the above mentioned password authentication protocols is utilised at least as far as management of the link between the user's terminal 1 and the network access server 4 is concerned.

This, for the purposes of the invention, would merely have the effect of providing a username and a dummy password associated with the user's terminal to the network access server 4.

Next, in a fourth step 23, the network access server 4 sends the associated authentication server 5 a message requesting access in respect of the user's terminal 1. This message will contain the number dialled by the user's terminal 1. This message will not however contain a password uniquely associated with the user's terminal 1 as required in these circumstances prior to the advent of the present invention. Whilst it is possible to deem the whole or a portion of the dialled telephone number to be an "effective password" , this cannot function as a password in the sense prevailing prior to the advent of the present invention as it cannot provide for a unique identification on a per user or per user's terminal basis.

In a fifth step 24, the authentication server 5 then checks to see if this dialled telephone number is one of one or more valid telephone numbers that are stored on the authentication server 5. As indicated above, these one or more valid telephone numbers will have been stored by prior arrangement and will be associated with either the point-of-presence operator itself or with a third party.

Thus if, for example, a dummy password had been passed to the network access server 4 from the user's terminal 1, this password would then be ignored for the purposes of the authentication process. Further, if, for example, a third party had reached a prior arrangement with the point-of-presence operator as indicated above, then the third party might have distributed connection service access software to potential customers of the connection service. This access software might have been pre-configured with a username corresponding to the third party. If this username had then been passed to the network access server 4, the point-of-presence could utilise the username to record usage information as to proportions of traffic originating with respective third party customers.

If the dialled telephone number is not one of the one or more valid telephone numbers then the connection has not been made on a valid telephone number and in a sixth step 25, the authentication server 5 returns a message to the network access server 4 that access is to be denied. In a seventh step 26, the user of the user's terminal 1 is informed that access has been denied by transmitting a message to the user's terminal 1.

If however the dialled telephone number is one of the one or more valid telephone numbers, then the connection has been received on a valid telephone number and in an eighth step 27, the authentication server 5 returns a message to the network access server 4 that access is to be allowed. In a ninth step 28, the network access server 4 then allocates an Internet Protocol network address to the user's terminal 1 and transmits this address to the user's terminal 1.

Finally, in a tenth step 29, the network access server 4 forms a connection between the user's terminal 1 and the Internet 6. The network access server 4 then permits messages to pass between the user's terminal 1 and the public Internet 6. Where such a message is being transmitted from the user's terminal 1 to the public Internet 6, it will contain the allocated Internet network address as the source address. Where the message is being passed from the public Internet 6 to the user's terminal 1, it will include the allocated Internet network address as the destination address. The user's computer can then transmit messages to other user's computers, such as the other user's computer 7 connected to the public Internet 6 using the Internet protocols mentioned above. The user's terminal 1 can also retrieve information pages from server computers, such as the server computer 8.

In an additional step in the authentication process, the network access server 4 may also ascertain the telephone number from which the user's terminal 1 placed the call. Such calling number functionality, commonly referred to as Calling Line Identity (CLI), will be known from the International Telegraph and Telephone Consultative Committee (CCITT) Common-Channel Signalling System No.7. The authentication server 5 may then, for example, compare the telephone number from which the user's terminal 1 placed the call with one or more stored telephone numbers which represent barred numbers. If the telephone number from which the user's terminal 1 placed the call is present on the list of such barred numbers then the authentication server 5 will not proceed to perform the authentication check on the basis of the telephone number which was dialled by the user's terminal 1. The authentication server 5 will instead return a message to the network access server 4 that access is to be denied. The network access server 4 may then send such an access denied message to the user's terminal 1. It will be appreciated that this pre-authentication check could instead test the number from which the user's terminal 1 made the call against a restricted group

of one or more numbers from which network access requests are allowed to be made. It will be further appreciated that the authentication process described above in terms of the dialled number (DNIS) could be carried out instead on the basis of the calling number (CLI).

The arrangement shown in Figure 1 is capable of providing more than one type of connection service. Each of these services may have its own dedicated telephone number.

In a basic service, the user's terminal 1 may be given general access to the public Internet 6. Where a user is using this basic service, the user of the user's terminal 1 may be charged at, for example, an ordinary local access rate for the use of the connection through the telephone network 2 to the point-of-presence 3. The user will be billed at this rate on the number from which the user's terminal placed the connection service access call by the telephone service billing system 9. Where the point-of-presence 3 and the telephone network 2 are owned by separate organisations, the telephone service billing system 9 may typically credit the owner of the Internet service provider with part of the call charge.

The arrangement shown in Figure 1 can also provide further services. Some information service providers require a payment for providing information. In a first further service, the network access server 4 provides access to one or a predefined set of server computers which provide information supplied by an information service provider and for which a payment is required. With this first further service, the call connection tariff includes a component to cover the payment required by the information service provider. The telephone service billing system 9 is arranged to credit part of the call charge to the information service provider. Thus, with this first further service, the user's terminal 1 gains access both to computers which can be accessed by general users of the Internet 6 as well as the one or predefined set of server computers mentioned above.

In a second further service, the user's terminal 1 may only be given access to one or a set of server computers which contain advertising material supplied by an information service provider. With this second service, the call tariff may be either at a reduced rate or a free rate with the information service provider paying some or all of the call charge. With this second service, the telephone service billing system 9 is arranged to charge the information service

provider for some or all of the call charge. Thus, with this second service, the user's terminal 1 gains access to just one server or to a set of servers which are restricted in comparison with the servers which can be accessed by general users of the Internet 6.

In further services, yet further arrangements of restricted or expanded access to network servers may be envisaged. Such further services may be effected, as above, through a specification of the network addresses to which an authenticated user's terminal 1 has access. Likewise further charging arrangements commensurate with further business models may also be envisaged. The connection time telephone network billing system element of the network access charge might, for example, be reduced to zero in the basic service, in favour of, for example, a fixed monthly charge.

Each such service or indeed the same or similar services offered by different operators may each have their own associated connection service access telephone number.

It is to be noted that authentication according to the invention can be performed not only in terms of the dialled telephone number (DNIS) and/or the dialling telephone number (CLI) but also on the basis of other attributes associated with the connection service access route. Examples of other such attributes include, for example, the Network Access Server IP address or the Network Access Server Identifier, indicating the network termination point. Similarly, when access technologies other than, for example, PSTN or ISDN, are utilised, the similarly associated access route attributes of a connection service based on this access technology can be used for such authentication.

Such associated access route attributes will share the above illustrated advantages associated with authentication on a dialled number. Again, all that will be required for access to the desired data network will be that the correct access route attribute be presented to the authentication server, in like fashion with the above illustrated embodiment where, rather than having to dial a valid connection telephone number and have further attributes checked (which might be subject to change, either deliberate or accidental, by a user), dialling a valid connection service telephone number will alone suffice for connection to the data network of choice.